6-2012

Non Interference for Intuitionist Necessity

Radha Jagadeesan
DePaul University, rjagadeesan@cs.depaul.edu

Corin Pitcher
DePaul University

James Riely
DePaul University

Non Interference for Intuitionist Necessity*

Radha Jagadeesan[1], Corin Pitcher[2], and James Riely[3]

1 **School of Computing**
College of CDM
DePaul University, Chicago,USA. rjagadeesan@cs.depaul.edu
2 **School of Computing**
College of CDM
DePaul University, Chicago,USA. cpitcher@cs.depaul.edu
3 **School of Computing**
College of CDM
DePaul University, Chicago,USA. jriely@cs.depaul.edu

Abstract

The necessity modality of intuitionist S4 is a comonad. In this paper, we study indexed necessity modalities that provide the logical foundation for a variety of applications; for example, to model possession of capabilities in policy languages for access control, and to track exceptions in type theories for exceptional computation.

Noninterference properties of the intuitionist logic of indexed necessity modalities capture the limitations on the information flow between formulas that are under the scope of necessity modalities with different indices. The impact of noninterference is seen in the unprovability of certain formulas. Noninterference is necessary for several applications. In models of capabilities, noninterference facilitates distributed reasoning. In models of exceptions, noninterference is necessary to ensure that the exceptions are tracked conservatively.

In this paper, we prove noninterference properties for indexed intuitionist necessity S4 modalities. To our knowledge, this is the first examination of noninterference results for the intuitionist S4 necessity modality (even without indexing).

1998 ACM Subject Classification F.4.1 Modal Logic

Keywords and phrases Intuitionist S4 necessity, comonad, noninterference, proof theory

Digital Object Identifier 10.4230/LIPIcs.xxx.yyy.p

1 Introduction

Classical S4 is standard textbook material, see for example the book by Hughes and Creswell [12]. The intuitionist versions of S4 are also well explored, e.g. [7, 16, 6, 11] to name but a few. We recall briefly. For any formula α, $\Box\alpha$ is also a formula. The necessity modality satisfies the following axioms.

N: necessitation. If α is a theorem, so is $\Box\alpha$
K: distribution. $\Box(\alpha \Rightarrow \beta) \Rightarrow \Box\alpha \Rightarrow \Box\beta$
T: reflexivity. $\Box\alpha \Rightarrow \alpha$
4: transitivity. $\Box\alpha \Rightarrow \Box\Box\alpha$

Clearly, this makes the necessity modality a comonad, so we use the terms comonad and necessity modality interchangeably.

* This work was partially supported by NSF CCF-0915704..

Conference title on which this volume is based on.
Editors: Billy Editor, Bill Editors; pp. 1–15

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

In this paper, we investigate the metatheory of indexed intuitionist S4 necessity modalities. Formally, let $(\mathscr{L}, \preceq)$ be a partial order. In several motivating examples, this partial order is a finite lattice. Let a, b, c range over principals. We consider a family of modalities, indexed by elements of $\mathscr{L}$, that support Principal naturality in addition to the the above axioms.

Necessity modality. For each $a \in \mathscr{L}$, $\Box_a(\cdot)$ is an S4 necessity modality, i.e. satisfies [N,K,4,T] above.

Principal Naturality. If $b \preceq a$, then $\Box_b \alpha \Rightarrow \Box_a \alpha$.

Such indexed necessity operators arise naturally in a variety of settings. We consider two examples from the literature below.

Security policy: In this example, the elements of the lattice are security principals. Principals are users, roles, locations or applications. The ordering in the lattice is the security order: if $b \preceq a$, then b is less secure than a. There is often a least secure principal and a most secure principal.

The indexed necessitation operator is used to capture the possession of capabiliities [9, 8]. We let object references (o, o') be atomic formulas. Then, $\Box_a o$ is intended to specify that a is permitted to possess the object reference o. $\Box_b o \Rightarrow o'$ specifies a guarded object (eg. a ciphertext). By necessitation (N), b gets the capability to the plaintext o' (specified as $\Box_a o'$) if it gets the key o (specified as $\Box_a o$).

In this application, principal naturality captures the idea that more secure principals have access to more capabilities.

Exceptional computations: The elements of the lattice are sets of exceptions. The ordering in the lattice is the subset order: i.e. $b \preceq a$ if $b \subseteq a$.

The necessity operator is used in the type theory to capture the names of the exceptions that can be raised in evaluating an expression [14, 13]. For example, consider $\Box_a \alpha$ for a modality-free intuitionist formula α. An expression has this type if the following hold: as usual, if its evaluation terminates normally, it results in a value of type ϕ; furthermore, any exception that it raises during an abnormal evaluation is contained in the set a. Thus, a is an upper bound on the exceptions that can be raised in evaluating an expression of this type; e.g., a pure functional program of type α that does not raise any exceptions is given the type $\Box_\emptyset \alpha$.

Relative to the traditional monadic view, it has been argued that this comonadic view of exceptions is more accurate (since exceptions are not first class values) and efficient (since it avoids tagging semantics) [14].

Since all types are (at least implicitly) under the scope of an indexed modality, axiom (T) plays a limited role in this treatment. Principal naturality is a conservative coercion that permits us to increase the upper bound on the set of exceptions that could be raised in evaluating an expression.

Noninterference.

Noninterference is the idea that there is no information flow between differently indexed modalities.

Let α be a modality free formula. Then, the intuitive idea behind non interference is that if $\Box_a \alpha$ is derivable from some hypothesis, then it is derivable from a subset of those hypothesis that are in the scope of the comonad indexed by a, i.e. the formulas of the form $\Box_a \cdot$. Thus, the logic does not permit assumptions made in the context of a principal b to affect the deductions in the context of a different principal a. Computations of values of a types are isolated from types that are not in the scope of an a indexed modality.

Noninterference implies the non provability of some simple formulas. Let p be a proposition, and $b \not\preceq a$. Then, the following formulas are not provable.

- $\not\vdash \Box_b p \Rightarrow \Box_a p$.

- $\not\vdash ((\Box_a p \Rightarrow q) \& \Box_b p) \Rightarrow \Box_a q$.

Noninterference is esential to justify the use of indexed necessity modalities in the modeling of both our motivating examples.

- The policies for capabilities are used in access control in a distributed system. The unprovability of $\Box_a p \Rightarrow \Box_b p$ ensures that the logical reasoning does not permit capabilities to be transferred in unrestrictedly between principals. The unprovability of $((\Box_a p \Rightarrow q) \& \Box_b p) \Rightarrow \Box_a q$ ensures that the acquiring of new capabilities (p) by another principal (b) does not create new capabilities for a principal (a) by purely logical reasoning.

  Thus, non-interference facilitates distribution and decentralized enforcement of policies in the following sense. The reference monitor at a location uses logical reasoning to deduce whether a principal has sufficient capabilities to access the resource available at the location. As discussed above, noninterference ensures that this reasoning is not dependent on other principals. This permits the reference monitor at a location to function without knowledge of the principals at other locations.
- In the modeling of exceptions, the consequences of noninterference are best seen in computational terms using the Curry-Howard isomorphism. The unprovability of the two formulas above captures the intuitive idea that there are no pure terms that can catch and handle the exceptions in $b \setminus a$. More generally, noninterference identifies the variables that can be queried during the evaluation of a pure expression in the scope of a $\Box_a \cdot$; clearly, any variable of a type $\Box_b \cdot$ cannot be queried if $a \not\sqsubseteq b$.

  Since there are no purely logical mechanisms to remove exceptions, that ability requires extra logical mechanisms, namely the exception handlers. For example, an exception handler that is catches *all* the exceptions in $a \setminus b$ and might only raise exceptions from b itself can be assigned the type $\Box_a \alpha \Rightarrow \Box_b \alpha$.

Results.

We describe a intuitionist logic with indexed necessity operators. Our sequent calculus is a multi-principal variant of the sequent calculus for intuitionist S4 described by Bierman and de Paiva [7].

Our statement of noninterference follows Abadi's statement for monadic logics [1]. We describe a translation of logical formulas into intuitionist propositional logic. This translation can be factored into two pieces:

Remove principals. The first piece translates formulas into a variant of the logic where the lattice has only one element. Thus, this component of the translation effectively yields a formula in a variant of Intutionist S4.

Erase modality. The standard forgetful translation from Intuitionist S4 into intutionist propositional logic that simply erases all modalities.

Both pieces are identity on intuitionist propositional logic.

The main technical result is that the translation preserve provability: i.e. if the source formula is a theorem in our logic (with indexed modalities), the target formula is provable in standard intuitionist propositional logic. This preservation validates the intuitive idea that the proof of a formula $\Box_a \alpha$ does not essentially use formulas that are *not* in the scope of $\Box_a \cdot$.

As simple illustrations of the power of this approach, we show how this result is used to establish the nonprovability of formulas, including the two unprovable formulas considered earlier in this introduction.

Our noninterference theorem has the formal form: "forall valid proofs. there exists a translated proof that is valid in intuitionist propositional logic". Thus, our results hold for *any* stricter logic that supports fewer proofs. To make our analysis more generally applicable, our variant of indexed

intuitionist S4 accommodates some of the natural variations can arise in application. Our design is guided by Abadi's formalization of the says monad [1] and games models thereof [5] .

We present two examples of the possible variations that we are able to accomodate. Consider the commutation of indexed modalities, i.e. is the sequent

$$\frac{}{\Box_b \Box_a \alpha \vdash \Box_a \Box_b \alpha}\ \text{(COMMUTATIVITY OF PRINCIPALS)}$$

provable? In addition to such extra commutativity principles, our logic also permits theorems such as:

$$(\alpha \Rightarrow \Box_a \beta) \Rightarrow \Box_a (\alpha \Rightarrow \Box_a \beta)$$

The above formula refers to only one lattice element, so is effectively a formula in intuitionist S4. It is however not a theorem in the standard presentation of the necessity modality of intuitionist S4.

Related work.

Classical S4 is standard textbook material [12]. Intuitionist S4 is also well explored, e.g Bierman and de Paiva [7] and Alechina, Mendler, de Paiva and Ritter [6] study categorical models of proof and provability. Pfenning and Wong [16] study the proof theory. We do not present a natural deduction system; the above papers discuss the subtle accommodations needed to facilitate the commutative conversions. Goubault-Larrecq and Goubault [11] study the geometry of the proofs of intuitionist S4 using tools from algebraic topology.

This prior work does not study principal-indexed comonads, and does not study non-interference.

There is an emerging literature that uses comonads to model coeffects as an alternative to effects and monads. Petricek, Orchard and Mycroft [15] aim to provide logical and type-theoretic foundations for this research program by associating information about context-dependence using comonads. Intuitively, the labels or tags on the comonad in the left hand side of a typing judgement represent constraints on the context in which the computation on the right is to be carried out. For example, in Nanevski [14] the tags on the context are the exceptions for which handlers are available. Contrast against the usual monadic approach that roughly propagates exceptions outwards. Malecha and Chong [13] also use the comonadic idea of moving exception handling capabilities from the outside to the inside.

Our exploration of noninterference results is inspired by the modelling of access control using "says" monads and the study of the metatheory of these logics [3, 4, 10, 1, 17]. Our proof of non-interference builds on the translation-based proof pioneered in this research [1, 17]. Our adaptation of these methods uses normal forms inspired by game semantics of monads [5]. This adaptation perforce has some new ingredients because comonads as not quite "dual" to monads. The dual of the comonad/necessity modality in classical S4 is the possibility modality and not the says modality; the possibility and says modalities differ in their distribution properties with respect to conjunction.

Rest of the paper.

In section 2 we describe a sequent calculus for the logic. The following section 3 describes our treatment of non interference. In section 4, we explicate the internal structure of our translations by a factorization result. We conclude in section 5.

2 Logic

We consider intuitionist propositional logic with indexed necessity modalities. Let $(\mathscr{L}, \preceq)$ be a partial order. Let a, b, c range over elements of $\mathscr{L}$. We consider a family of modalities that are

indexed by elements of $\mathscr{L}$. We include conjunction and implication but not disjunction.

Formulas are defined inductively by:

$$\begin{array}{lll} \alpha,\beta,\gamma ::= \mathtt{tt} & & \text{(True)} \\ \quad \mid p,q & & \text{(Propositional Variables)} \\ \quad \mid \alpha \& \beta & & \text{(Conjunction)} \\ \quad \mid \alpha \Rightarrow \beta & & \text{(Implication)} \\ \quad \mid \Box_a \alpha & & \text{(Comonad)} \end{array}$$

2.1 a-available

The following definition impacts the comonad introduction rule on the right. Formally, the format of the definition shadows Abadi's treatment in logics for monads [1].

Definition 1. a-available formulas are inductively defined as follows.

- $\mathtt{tt}$ is a-available.
- $\Box_b \alpha$ is a-available if $b \preceq a$
- If α is a-available, so are $(\beta \Rightarrow \alpha)$, $\forall p.\alpha$, and $\Box_b \alpha$.
- If α, β are a-available, so is $(\alpha \& \beta)$.

This definition extends to sets/multisets/sequences of formulas $\Gamma = \alpha_1 \dots \alpha_n$ pointwise. $\Gamma = \alpha_1, \dots, \alpha_n$ is a-available if all $\alpha_1, \dots, \alpha_n$ are a-available. □

It will turn out that an a-available formula α is one that satisfies $\alpha \Rightarrow \Box_a \alpha$. In standard presentations, these are the formulas of form $\Box_a \cdot$. We motivate our more liberal presentation using game semantics [5] [1]. From this perspective, a formula is a-available if the first move in the game happens in the context of a principal lower in $\preceq$ than a. Thus, $\Box_b \alpha$ is a-available if $b \preceq a$ or α is a-available. $\mathtt{tt}$ is a-available since it has no moves. The first move in $(\beta \Rightarrow \alpha)$ comes from α, so it is a-available if α is. The first moves of $(\alpha \& \beta)$ comes from either α or β, so it is a-available if both α, β are.

Lemma 2. If $b \preceq a$ and α is b-available, then α is b-available. □

PROOF. Proof by induction on structure of formulas. The proof of base case for $\Box_a \cdot$ formulas uses the transitivity of $\preceq$. □

2.2 Sequent calculus

The sequent calculus for the logic is given in Figure 1. Our sequent calculus is a multi-principal variant of the necessity fragment of the sequent calculus of Bierman and De Paiva [7]. The only modification is in the PROMOTE rule that uses our more generous variation of a-available.

Remark 3 (Weakening). Weakening is admissible [7]. This is the motivation for the weakening built into AXIOM and PROMOTE. □

Remark 4 (Cut). Cut is admissible. In this paper, we do not discuss cut-elimination any further, whose proofs follow the standard outline laid out for the sequent calculus for intiutionist S4 [7]. □

[1] Abramsky and Jagadeesan [5] describe game semantics for monads in a form that is easily adapted to comonads. Merely invert the inequality in the definition of condition (p6) in that paper.

$$\frac{}{\Gamma,\alpha\vdash\ \alpha}\ (\text{AXIOM})$$

$$\frac{\Gamma\vdash\ \alpha \qquad \Delta,\alpha\vdash\ \beta}{\Gamma,\Delta\vdash\ \beta}\ (\text{CUT})$$

$$\frac{\Gamma,\gamma,\beta,\Delta\vdash\ \alpha}{\Gamma,\beta,\gamma,\Delta\vdash\ \alpha}\ (\text{EXCHANGE})$$

$$\frac{\Gamma\vdash\ \alpha}{\Gamma,\beta\vdash\ \alpha}\ (\text{WEAKENING})$$

$$\frac{\Gamma,\beta,\beta,\Delta\vdash\ \alpha}{\Gamma,\beta,\Delta\vdash\ \alpha}\ (\text{CONTRACTION})$$

$$\frac{\Gamma,\beta,\gamma,\Delta\vdash\ \alpha}{\Gamma,\beta\&\gamma,\Delta\vdash\ \alpha}\ (\&\text{-L})$$

$$\frac{\Gamma\vdash\ \alpha \qquad \Gamma\vdash\ \beta}{\Gamma\vdash\ \alpha\&\beta}\ (\&\text{-R})$$

$$\frac{\Gamma\vdash\ \alpha}{\Gamma,\texttt{tt}\vdash\ \alpha}\ (\texttt{tt}\text{-L})$$

$$\frac{}{\Gamma\vdash\ \texttt{tt}}\ (\texttt{tt}\text{-R})$$

$$\frac{\Gamma,\beta\vdash\ \gamma}{\Gamma\vdash\ \beta\Rightarrow\gamma}\ (\Rightarrow\text{-R})$$

$$\frac{\Gamma\vdash\ \beta \qquad \Gamma,\gamma\vdash\ \alpha}{\Gamma,\beta\Rightarrow\gamma\vdash\ \alpha}\ (\Rightarrow\text{-L})$$

$$\frac{\Gamma,\beta\vdash\ \alpha}{\Gamma,\Box_a\beta\vdash\ \alpha}\ (\text{COUNIT})$$

$$\frac{\Gamma\vdash\ \alpha}{\Gamma,\Delta\vdash\ \Box_a\alpha}\ \Gamma\ a-available\ (\text{PROMOTE})$$

Figure 1 Sequent calculus

Remark 5 (Natural deduction). We do not present a natural deduction system;. Subtle accommodations are needed to facilitate the commutative conversions, see [7] and [16]. □

Remark 6 (Standard theorems). The standard ingredients for intuitionist necessity are derivable standardly. *None* of the following derivations use the third or fourth cases of the definition 1.

$$\frac{}{\Box_a\alpha\vdash\ \Box_a\Box_a\alpha}\ (\text{COMULTIPLICATION})$$

is derived using AXIOM on $\Box_a\alpha$ followed by PROMOTE.

$$\frac{\beta\vdash\ \alpha}{\Box_a\beta\vdash\ \Box_a\alpha}\ (\text{FUNCTORIALITY})$$

is derived using cut against COUNIT followed byPROMOTE.

The coercion from lesser principals to greater principals.

$$\frac{}{\Box_b\alpha\vdash\ \Box_a\alpha}\ b\preceq a\ (\text{PRINCIPAL NATURALITY})$$

is derivable starting with AXIOM on α, using cut against COUNIT (on b) followed by PROMOTE. □

Remark 7. (Non standard theorems) Sequences of nested comonads without intervening connectives can be exchanged:

$$\frac{}{\Box_b\Box_a\alpha\vdash\ \Box_a\Box_b\alpha}\ (\text{COMMUTATIVITY OF PRINCIPALS})$$

COUNIT yields $\Box_a\Box_b\alpha \vdash \ \alpha$. The second case of definition 1 ensures that $\Box_a\Box_b\alpha$ is a-available, so use of PROMOTE yields $\Box_a\Box_b\alpha \vdash \ \Box_a\alpha$. The *third* case of definition 1 ensures that $\Box_a\Box_b\alpha$ is b-available, so use of PROMOTE yields the required result. Thus, for a set of principals $\mathscr{S} = \{a,b,c,\ldots..\}$, using commutativity of principals we could define without ambiguity:

$$\Box_{\mathscr{S}}\alpha \triangleq \Box_a\Box_b\Box_c\ldots\alpha$$

Another nonstandard new theorem is:

$$\overline{\alpha \Rightarrow \Box_a\beta \vdash \ \Box_a(\alpha \Rightarrow \Box_a\beta)}$$

Start with AXIOM on $\alpha \Rightarrow \Box_a\beta$. The *third* case of definition 1 ensures that $\alpha \Rightarrow \Box_a\beta$ is a-available since $\Box_a\beta$ is, so use of PROMOTE yields the required result. □

Remark 8 (Unprovable formulas).

$$\begin{array}{l} p \vdash \ \Box_a p \ \text{ is not provable} \\ \Box_b p \vdash \ \Box_a p \ \text{ is not provable if } b \not\preceq a \end{array}$$

Thus, $\Box_a p$ and $\Box_b p$ are in general unrelated versions of p. However, both are always stronger than the undecorated proposition p.

$$\Box_b p, \Box_a(p \Rightarrow q) \vdash \ \Box_a q \ \text{ is not provable if } b \not\preceq a$$

So, necessitation (N) does not hold across multiple principals. □

Remark 9 (Kripke semantics: an attempt). To gain more insight, consider a partial attempt at Kripke models for the logic, building on Goubault-Larrecq and Gobault [11]. An indexed intuitionist Kripke frame $(W, \{\rhd_a \mid a \in \mathscr{L}\}, \geq)$ is a set of worlds (W), where each $\rhd_a$ and $\geq$ are preorders on W satisfying:

- $(\forall a) \ \ \geq \subseteq \rhd_a$
- If $b \preceq a$ then $\rhd_b \supseteq \rhd_a$
- If $(\forall a,b) \ \ \rhd_a;\rhd_b = \rhd_b;\rhd_a$

The first condition follows Goubault–Larrecq and Gobault [11], who adapt Wolter and Zakharyashev [18]. The second condition accounts for principal naturality. The third condition accounts for the commutativity of the different indices.

As standard, valuations assign $\geq$-closed sets to propositions. The traditional intuitionist semantics is used for all intuitionist connectives, and the indexed $\rhd_a$ is used to evaluate indexed $\Box_a\cdot$ necessity formulas standardly. Validity is as usual.

Alas, this attempt is uanble to account for the fact that $\alpha \Rightarrow \beta$ is a-available if β is a-available!□

3 Non-interference

In this section, we establish non-interference theorems for the logic.

3.1 Normal forms

Our proofs rely on normal forms for formulas. These normal forms are inspired by game semantics. A unique result formula is one whose game *has* a unique starting move. A multiple result formula

is one which *may* have multiple starting moves. In syntatic terms, a unique result formula does not have any conjunction at the ultimate result type.

$$\delta ::= \mathtt{tt} \mid p, q \mid \mu \Rightarrow \delta \mid \Box_a \delta \mid \forall p.\delta \qquad \text{(Unique result formulas)}$$
$$\mu ::= \delta \mid \mu \& \delta \mid \delta \& \mu \qquad \text{(Multiple result formulas)}$$

Any formula α is equivalent to a multiple result formula. This is proved by using the following distributivity laws:

$$\begin{array}{lcl} \Box_a(\alpha \& \beta) & \Leftrightarrow & \Box_a \alpha \& \Box_a \beta \\ \alpha \Rightarrow (\beta \& \gamma) & \Leftrightarrow & (\alpha \Rightarrow \beta) \& (\alpha \Rightarrow \gamma) \end{array}$$

Remark 10. Multiple result formulas are closed under the subformula property. So, in light of cut elimination, the earlier sequent calculus specializes down to one restricted to multiple result formulas. □

In the rest of this section, without loss of generality, we will assume that all the formulas are multiple result formulas.

3.2 Translations of formulas

We describe two translations $\langle \alpha \rangle_a^+$ and $\langle \alpha \rangle_a^-$ on multiple-result formulas by mutual recursion. Both translations yield pure IPL formulas without any comonads. The translation $\langle \cdot \rangle_a^-$ is closest in spirit to the extant treatment of the says monad [1], albeit with modifications designed to accommodate the differences arising from the comonad. In section 4, we discuss a factorization of the translation.

Both translations share some common features. Both are structural and remove all modalities. Both translations "delete" some information by replacing some chosen subformulas by $\mathtt{tt}$.

The intuition is that both translations try to ensure that results of a-available formulas are not influenced by formulas that are not a-available. This is illustrated by considering the translation of $\alpha \Rightarrow \beta$ when β is a-available. In this case, the translations ensure that all the subformulas of α that are not a-available are replaced by $\mathtt{tt}$. Viewing via the lens of game semantics, the translations replace the non a-available formulas by the empty game that interprets $\mathtt{tt}$. Thus, the Opponent cannot move in these subformula occurrences. What the following preservation theorem 17 shows is that the proof also does not need to make moves in this proposition instance, i.e. this subformula instance is expendable to the proof.

$\langle \cdot \rangle_a^-$ enforces more constraints: it also replaces the results that are not a-available by $\mathtt{tt}$.

Definition 11. For a formula α in multiple result normal form, define $\langle \alpha \rangle_a^+, \langle \alpha \rangle_a^-$ in IPL as follows.

$$\begin{array}{ll|ll} \langle \mathtt{tt} \rangle_a^+ & = \mathtt{tt} & \langle \mathtt{tt} \rangle_a^- & = \mathtt{tt} \\ \langle p \rangle_a^+ & = p & \langle p \rangle_a^- & = \mathtt{tt} \\ \langle \alpha \& \beta \rangle_a^+ & = \langle \alpha \rangle_a^+ \& \langle \beta \rangle_a^+ & \langle \alpha \& \beta \rangle_a^- & = \langle \alpha \rangle_a^- \& \langle \beta \rangle_a^- \\ \langle \Box_b \alpha \rangle_a^+ & = \langle \alpha \rangle_a^+ & \langle \Box_b \alpha \rangle_a^- & = \begin{cases} \langle \alpha \rangle_a^-, & b \not\preceq a \\ \langle \alpha \rangle_a^+, & b \preceq a \end{cases} \\ \langle \alpha \Rightarrow \beta \rangle_a^+ & = \begin{cases} \langle \alpha \rangle_a^- \Rightarrow \langle \beta \rangle_a^+, & \beta \ a-\text{available} \\ \langle \alpha \rangle_a^+ \Rightarrow \langle \beta \rangle_a^+, & \text{otherwise} \end{cases} & \langle \alpha \Rightarrow \beta \rangle_a^- & = \langle \alpha \rangle_a^- \Rightarrow \langle \beta \rangle_a^- \end{array}$$

These definitions extend to sets/multisets/sequences of formulas $\Gamma = \alpha_1 \ldots \alpha_n$ pointwise.

$$\begin{array}{l} \langle \Gamma \rangle_a^+ = \langle \alpha_1 \rangle_a^+, \ldots, \langle \alpha_n \rangle_a^+ \\ \langle \Gamma \rangle_a^- = \langle \alpha_1 \rangle_a^-, \ldots, \langle \alpha_n \rangle_a^+ \end{array}$$

□

Consider propositions p. $\langle p\rangle_a^+$ is p since there are no isolation constraints that need to be enforced. However, since p is not a-available, $\langle p\rangle_a^-$ is $\mathtt{tt}$.

$\langle\cdot\rangle_a^+$ is fully compositional for all cases except implication $\alpha \Rightarrow \beta$ when β is a-available. In this case, we switch to $\langle\alpha\rangle_a^-$to ensure that only a-available formulas influence a-available results.

$\langle\cdot\rangle_a^-$ is fully compositional for all cases except $\Box_b\alpha$ when $b \preceq a$. In this case, we switch to $\langle\alpha\rangle_a^+$ because the the enclosing comonad $\Box_b\cdot$ intuitively has already discharged the constraint of making the formula available to a, so we only need to enforce the constraints of $\langle\cdot\rangle_a^+$.

Example 12.

$$\begin{aligned}&\langle p \Rightarrow q\rangle_a^+ = p \Rightarrow q\\ &\langle p \Rightarrow q\rangle_a^- = \mathtt{tt}\\ &\langle p \Rightarrow \Box_a q\rangle_a^+ = \langle p \Rightarrow \Box_a q\rangle_a^- = \mathit{true} \Rightarrow q\end{aligned}$$ □

Remark 13. The translations described above are not semantically robust. They do not respect equivalence of formulas. They have the desired properties explicated below only on formulas in multiple result normal form. □

The translations coincide on a-available formulas. This confirms the intuition that they differ only in the availability of the top-level formula.

Lemma 14. If α is a-available, then $\langle\alpha\rangle_a^+ = \langle\alpha\rangle_a^-$. □

PROOF. By structural induction on α. The base cases for the induction are when α is of the form $\mathtt{tt}$ and $\Box_b\beta$ with $b \preceq a$. In these cases, $\langle\alpha\rangle_a^+ = \langle\alpha\rangle_a^-$ by definition.

If β, γ are a-available:

$$\begin{aligned}\langle\beta\&\gamma\rangle_a^+ &= \langle\beta\rangle_a^+ \& \langle\gamma\rangle_a^+\\ &= \langle\beta\rangle_a^- \& \langle\gamma\rangle_a^-\\ &= \langle\beta\&\gamma\rangle_a^-\end{aligned}$$

If γ is a-available:

$$\begin{aligned}\langle\beta \Rightarrow \gamma\rangle_a^+ &= \langle\beta\rangle_a^- \Rightarrow \langle\gamma\rangle_a^+\\ &= \langle\beta\rangle_a^- \Rightarrow \langle\gamma\rangle_a^-\\ &= \langle\beta \Rightarrow \gamma\rangle_a^-\end{aligned}$$

If $b \not\preceq a$ and β is a-available:

$$\begin{aligned}\langle\Box_b\beta\rangle_a^+ &= \langle\beta\rangle_a^+\\ &= \langle\beta\rangle_a^-\\ &= \langle\Box_b\beta\rangle_a^-\end{aligned}$$

If β is a-available:

$$\begin{aligned}\langle\forall p.\beta\rangle_a^+ &= \forall p.\langle\beta\rangle_a^+\\ &= \forall p.\langle\beta\rangle_a^-\\ &= \langle\forall p.\beta\rangle_a^-\end{aligned}$$ □

The next two lemmas are the key technical drivers that motivate the consideration of normal forms for formulas in this proof. If the sole result of a single result formula is not a-available, the $\langle\cdot\rangle_a^-$ translation removes all non trivial information from it.

Lemma 15. If a single result formula δ is not a-available, then $\langle\delta\rangle_a^- = \mathtt{tt}$. □

PROOF. By structural induction on δ. If δ is of the form $\mathtt{tt}$ or p, $\langle\delta\rangle_a^- = \mathtt{tt}$ by definition.

If δ is not a-available, for any α

$$\begin{aligned}\langle\alpha \Rightarrow \delta\rangle_a^- &= \langle\alpha\rangle_a^- \Rightarrow \langle\delta\rangle_a^- \\ &= \langle\alpha\rangle_a^- \Rightarrow \mathtt{tt} \\ &= \mathtt{tt}\end{aligned}$$

If $b \not\preceq a$ and δ is not a-available:

$$\begin{aligned}\langle\Box_b\delta\rangle_a^- &= \langle\delta\rangle_a^- \\ &= \mathtt{tt}\end{aligned}$$

If δ is not a-available:

$$\begin{aligned}\langle\forall p.\delta\rangle_a^- &= \forall p.\langle\delta\rangle_a^- \\ &= \forall p.\mathtt{tt} \\ &= \mathtt{tt}\end{aligned}$$

□

We are now able to confirm that the $\langle\cdot\rangle_a^-$ translation is more restrictive than the $\langle\cdot\rangle_a^+$ translation.

Lemma 16. For all μ in multiple result form , $\langle\mu\rangle_a^+ \vdash \langle\mu\rangle_a^-$ is provable. □

PROOF. *Single Result Formulas:* Consider first the case when μ is a formula δ in single result form. We prove the result by structural induction on the construction of δ.

If δ is of the form $\mathtt{tt}$ or p. In these cases, result follows since $\langle\delta\rangle_a^- = \mathtt{tt}$.

If δ is a-available:

$$\begin{aligned}\langle\beta \Rightarrow \delta\rangle_a^+ &= \langle\beta\rangle_a^- \Rightarrow \langle\delta\rangle_a^+ \\ &\Rightarrow \langle\beta\rangle_a^- \Rightarrow \langle\delta\rangle_a^- \\ &= \langle\beta \Rightarrow \delta\rangle_a^-\end{aligned}$$

If δ is not a-available, $\beta \Rightarrow \delta$ is not a-available and result follows since $\langle\beta \Rightarrow \gamma\rangle_a^- = \mathtt{tt}$ by lemma 15.

If $b \not\preceq a$:

$$\begin{aligned}\langle\Box_b\delta\rangle_a^+ &= \langle\delta\rangle_a^+ \\ &\Rightarrow \langle\delta\rangle_a^- \\ &= \langle\Box_b\delta\rangle_a^-\end{aligned}$$

If $b \preceq a$:

$$\begin{aligned}\langle\Box_b\delta\rangle_a^+ &= \langle\delta\rangle_a^+ \\ &= \langle\Box_b\delta\rangle_a^-\end{aligned}$$

For the case of the quantifier:

$$\begin{aligned}\langle\forall p.\delta\rangle_a^+ &= \forall p.\langle\delta\rangle_a^+ \\ &\Rightarrow \forall p.\langle\delta\rangle_a^- \\ &= \langle\forall p.\delta\rangle_a^-\end{aligned}$$

Multiple result formulas. Given the result for single-result formulas, the proof for multiple result formulas μ follows by structural induction on the formation of μ. □

3.3 Noninterference

The translations preserve provability.

Theorem 17. Let Γ, α be formulas in multiple result form. If $\Gamma \vdash \alpha$, then:

- $\langle\Gamma\rangle_a^+ \vdash \langle\alpha\rangle_a^+$, *and*
- $\langle\Gamma\rangle_a^- \vdash \langle\alpha\rangle_a^-$

are provable in intuitionist propositional logic. □

PROOF. Proof by induction on the structure of the proof of $\Gamma \vdash \alpha$.

We first prove the induction step for $\langle\Gamma\rangle^-_a \vdash \langle\alpha\rangle^-_a$.

- The proofs for the inductive case when the last rule is any rule except COUNIT or PROMOTE are all similar. In each of these cases, the inductive step to show $\langle\Gamma\rangle^-_a \vdash \langle\alpha\rangle^-_a$ follows because the translation $\langle(\cdot)\rangle^-_a$ is compositional on the structure of the propositional connectives and the universal quantifier.
  For example consider the case when the last step in the proof of $\Gamma \vdash \alpha$ is &-R. So, we have $\alpha = \beta\&\gamma$ and the following proof structure:

$$\frac{\Gamma \vdash \beta \qquad \Gamma \vdash \gamma}{\Gamma \vdash \beta\&\gamma}$$

  By inductive hypothesis, we deduce a proof of $\langle\Gamma\rangle^-_a \vdash \langle\beta\rangle^-_a$ and $\langle\Gamma\rangle^-_a \vdash \langle\gamma\rangle^-_a$. An application of &-R yields $\langle\Gamma\rangle^-_a \vdash \langle\beta\rangle^-_a\&\langle\gamma\rangle^-_a$ thus completing this case since $\langle\alpha\rangle^-_a = \langle\beta\rangle^-_a\&\langle\gamma\rangle^-_a$.
- If the last rule is COUNIT, i.e.

$$\frac{\Gamma, \beta \vdash \alpha}{\Gamma, \Box_b\beta \vdash \alpha}\ \text{(COUNIT)}$$

  by induction hypothesis, we have a proof of

$$\langle\Gamma\rangle^-_a, \langle\beta\rangle^-_a \vdash \langle\alpha\rangle^-_a$$

  There are two cases depending on the order between b, a.
  $b \preceq a$ By definition, $\langle\Box_b\beta\rangle^-_a = \langle\beta\rangle^+_a$. From lemma 16, $\langle\beta\rangle^+_a \vdash \langle\beta\rangle^-_a$ is provable, so we get required result by use of CUT with the proof above yielded by the induction hypothesis.
  $b \not\preceq a$. By definition, $\langle\Box_b\beta\rangle^-_a = \langle\beta\rangle^-_a$. Hence, the induction hypothesis yields the required result.
- If the last rule is PROMOTE, i.e.

$$\frac{\Gamma \vdash \alpha}{\Gamma \vdash \Box_b\alpha}\ \Gamma\ is\ b-available\ \text{(PROMOTE)}$$

  There are two cases depending on the order between b, a.
  $b \preceq a$ By induction hypothesis on the $\langle\cdot\rangle^+_a$ translation, we have a proof of

$$\langle\Gamma\rangle^+_a \vdash \langle\alpha\rangle^+_a$$

  Since $b \preceq a$, by lemma 2, Γ is also a-available. So, by lemma 14, $\langle\Gamma\rangle^+_a = \langle\Gamma\rangle^-_a$. Also, by definition, $\langle\Box_b\alpha\rangle^-_a = \langle\alpha\rangle^+_a$.
  $b \not\preceq a$. By induction hypothesis, we have a proof of

$$\langle\Gamma\rangle^-_a \vdash \langle\alpha\rangle^-_a$$

  By definition, $\langle\Box_b\alpha\rangle^-_a = \langle\alpha\rangle^-_a$.
  In either case, the required proof of

$$\langle\Gamma\rangle^-_a \vdash \langle\Box_b\alpha\rangle^-_a$$

  coincides with the proof yielded by induction hypothesis and the additional formulas Δ on the left are added using weakening.

We next prove the induction step for $\langle\Gamma\rangle^+_a \vdash \langle\alpha\rangle^+_a$.

- The translation $\langle(\cdot)\rangle_a^+$ is compositional on the structure of &, comonad and the universal quantifier. So, if the last rule is any except $\Rightarrow$-R or $\Rightarrow$-L, the inductive step to show that $\langle\Gamma\rangle_a^+ \vdash \langle\alpha\rangle_a^+$ holds follows immediately.
  For example, consider the case when the last step in the proof of $\Gamma \vdash \alpha$ is &-R. So, we have $\alpha = \beta\&\gamma$ and the following proof structure:

$$\frac{\Gamma \vdash \beta \qquad \Gamma \vdash \gamma}{\Gamma \vdash \beta\&\gamma}$$

  By inductive hypothesis, we deduce a proof of $\langle\Gamma\rangle_a^+ \vdash \langle\beta\rangle_a^+$ and $\langle\Gamma\rangle_a^+ \vdash \langle\gamma\rangle_a^+$. An application of &-R yields $\langle\Gamma\rangle_a^+ \vdash \langle\beta\rangle_a^+\&\langle\gamma\rangle_a^+$. This completes this caseof the proof since $\langle\alpha\rangle_a^+ = \langle\beta\rangle_a^+\&\langle\gamma\rangle_a^+$.
- If the last rule is $\Rightarrow$-R or $\Rightarrow$-L and the implication formula in question is $\beta \Rightarrow \gamma$, there are two cases based on whether γ is a-available or not.
  If γ is not a-available, the $\langle\cdot\rangle_a^+$ translation is still compositional, i.e. $\langle\beta \Rightarrow \gamma\rangle_a^+ = \langle\beta\rangle_a^+ \Rightarrow \langle\gamma\rangle_a^+$ and the proof is similar to case above.
  If γ is a-available, $\langle\beta \Rightarrow \gamma\rangle_a^+ = \langle\beta\rangle_a^- \Rightarrow \langle\gamma\rangle_a^+$.
  $\Rightarrow$-R: The last rule is:

$$\frac{\Gamma, \beta \vdash \gamma}{\Gamma \vdash \beta \Rightarrow \gamma}\ (\Rightarrow\text{-R})$$

  From induction hypothesis, we deduce the existence of a proof of

$$\langle\Gamma\rangle_a^-, \langle\beta\rangle_a^- \vdash \langle\gamma\rangle_a^-$$

  and hence a proof for

$$\langle\Gamma\rangle_a^- \vdash \langle\beta \Rightarrow \gamma\rangle_a^-$$

  since $\langle\beta \Rightarrow \gamma\rangle_a^- = \langle\beta\rangle_a^- \Rightarrow \langle\gamma\rangle_a^-$. Since $\beta \Rightarrow \gamma$ is a-available, $\langle\beta \Rightarrow \gamma\rangle_a^- = \langle\beta \Rightarrow \gamma\rangle_a^+$ by lemma 14. So, we deduce a proof for:

$$\langle\Gamma\rangle_a^- \vdash \langle\beta \Rightarrow \gamma\rangle_a^+$$

  From lemma 16, the sequents $\langle\alpha\rangle_a^+ \vdash \langle\alpha\rangle_a^-$ are provable for each $\alpha \in \Gamma$. So, by multiple uses of cut, we get a proof of:

$$\langle\Gamma\rangle_a^+ \vdash \langle\beta \Rightarrow \gamma\rangle_a^+$$

  as required.
  $\Rightarrow$-L: The last rule is:

$$\frac{\Gamma \vdash \beta \qquad \Gamma, \gamma \vdash \alpha}{\Gamma, \beta \Rightarrow \gamma \vdash \alpha}\ (\Rightarrow\text{-L})$$

  From induction hypothesis, we deduce the existence of proofs of

$$\langle\Gamma\rangle_a^- \vdash \langle\beta\rangle_a^-$$

  and

$$\langle\Gamma\rangle_a^+, \langle\gamma\rangle_a^+ \vdash \langle\alpha\rangle_a^+$$

  From lemma 16, the sequents $\langle\alpha\rangle_a^+ \vdash \langle\alpha\rangle_a^-$ are provable for each $\alpha \in \Gamma$. So, by multiple uses of cut with the first proof, we get a proof of:

$$\langle\Gamma\rangle_a^+ \vdash \langle\beta\rangle_a^-$$

Using $\Rightarrow$-L withthe second proof above yields a proof of:

$$\langle\Gamma\rangle_a^+, \langle\beta\rangle_a^- \Rightarrow \langle\gamma\rangle_a^+ \vdash \langle\alpha\rangle_a^+$$

Required result follows since $\langle\beta \Rightarrow \gamma\rangle_a^+ = \langle\beta\rangle_a^- \Rightarrow \langle\gamma\rangle_a^+$. □

The main use of this theorem is to prove that certain sequents are not provable. We illustrate with very simple examples.

Example 18. In all the following examples, we use theorem 17 for $\langle\cdot\rangle_a^-$.

- If the sequent $p \vdash \Box_a p$ is provable, so would $\mathtt{tt} \vdash p$. Hence, $p \vdash \Box_a p$ is not provable.
- Let $b \not\preceq a$. If the sequent $\Box_b p \vdash \Box_a p$ is provable , so would $\mathtt{tt} \vdash p$ in IPL. Hence $\Box_b p \vdash \Box_a p$, is not provable.
- Let $b \not\preceq a$. Then if the sequent $\Box_b p, \Box_a p \Rightarrow q \vdash \Box_a q$ is provable, so would $\mathtt{tt}, p \Rightarrow q \vdash q$. Hence, $\Box_b p, \Box_a p \to q \vdash \Box_a q$ is not provable.

4 Factoring the translation

We chose to present the results for the unfactored translation first in order to emphasize that our *proof* of theorem 17 is not dependent on the vagaries of the source modal logic.

The translations $\langle\cdot\rangle_a^+$ and $\langle\cdot\rangle_a^-$ can be factored into two pieces:

Remove principals. Translations $(|\cdot|)_a^+$ and $(|\cdot|)_a^-$ into the fragment of our logic that uses modalities indexed only by a. Thus, the target of this translation is a variant of Intutionist S4.

Erase modality. The standard forgetful translation from Intuitionist S4 into intutionist propositional logic that simply erases all modalities.

Concretely, for a formula α in multiple result normal form, define $(|\alpha|)_a^+, (|\alpha|)_a^-$ as follows. The only differences are in the cases for the modality.

$$\begin{array}{ll|ll}
(|\mathtt{tt}|)_a^+ & = \mathtt{tt} & (|\mathtt{tt}|)_a^- & = \mathtt{tt} \\
(|p|)_a^+ & = p & (|p|)_a^- & = \mathtt{tt} \\
(|\alpha\&\beta|)_a^+ & = (|\alpha|)_a^+ \& (|\beta|)_a^+ & \langle\alpha\&\beta\rangle_a^- & = (|\alpha|)_a^- \& (|\beta|)_a^- \\
(|\Box_b\alpha|)_a^+ & = \begin{cases} (|\alpha|)_a^+, & b \not\preceq a \\ \Box_a(|\alpha|)_a^+, & b \preceq a \end{cases} & (|\Box_b\alpha|)_a^- & = \begin{cases} (|\alpha|)_a^-, & b \not\preceq a \\ \Box_a(|\alpha|)_a^+, & b \preceq a \end{cases} \\
(|\alpha \Rightarrow \beta|)_a^+ & = \begin{cases} (|\alpha|)_a^- \Rightarrow \langle\beta\rangle_a^+, & \beta\ a-\text{available} \\ (|\alpha|)_a^+ \Rightarrow \langle\beta\rangle_a^+, & \text{otherwise} \end{cases} & \langle\alpha \Rightarrow \beta\rangle_a^- & = \langle\alpha\rangle_a^- \Rightarrow \langle\beta\rangle_a^-
\end{array}$$

We are able to prove the analogue of theorem 17. If $\Gamma \vdash \alpha$, then:

- $(|\Gamma|)_a^+ \vdash (|\alpha|)_a^+$, and
- $(|\Gamma|)_a^- \vdash (|\alpha|)_a^-$

are provable. The proof uses the analogues for lemmas 14— 16 that are listed below.

1. If α is a-available, then $(|\alpha|)_a^+ = (|\alpha|)_a^-$; furthermore, $(|\alpha|)_a^+$ is a-available.
2. If a single result formula δ is not a-available, then $(|\delta|)_a^- = \mathtt{tt}$.
3. For all μ in multiple result form , $(|\mu|)_a^+ \vdash (|\mu|)_a^-$ is provable.

Note the extra conclusion in the first item relative to lemma 14. Given this, the proof that the translations preserve provability follows the proof of theorem 17 exactly. The only case that is different is the inductive case of PROMOTE for $(|\cdot|)_a^-$. We present the proof for this case below. If the last rule is PROMOTE, i.e.

$$\frac{\Gamma \vdash \alpha}{\Gamma \vdash \Box_b\alpha}\ (\text{PROMOTE})\ \Gamma \textit{ is } b-\textit{available}$$

There are two cases depending on the order between b, a.

$b \preceq a$ By induction hypothesis on the $(|\cdot|)^+_a$ translation, we have a proof of

$$(|\Gamma|)^+_a \vdash (|\alpha|)^+_a$$

Since $b \preceq a$, by lemma 2, Γ is also a-available. So, by first item above, $(|\Gamma|)^+_a = (|\Gamma|)^-_a$. Also, by definition, $(|\Box_b \alpha|)^-_a = \Box_a (|\alpha|)^+_a$. The required proof of

$$(|\Gamma|)^-_a \vdash \Box_a (|\alpha|)^-_a$$

is yielded by PROMOTE on the proof yielded by induction hypothesis. PROMOTE is permissible since by first item above, $(|\Gamma|)^-_a$ is a-available.

$b \not\preceq a$. By induction hypothesis, we have a proof of

$$(|\Gamma|)^-_a \vdash (|\alpha|)^-_a$$

By definition, $(|\Box_b \alpha|)^-_a = (|\alpha|)^-_a$. In this case, the required proof is yielded by the induction hypothesis.

The proof for the translations $(|\cdot|)^+_a, (|\cdot|)^-_a$ that are presented in this section depend more delicately on the source modal logic, as is revealed in the precise use of the format of the PROMOTE rule above.

5 Conclusions

Recent research in both type theories and security have used indexed necessity modalities (ie. comonads) of intuitionist S4 as the logical foundations. A key metathoretic property that is essential to the soundness of this modeling is noninterference between the different indices. In this paper, we establish noninterference for indexed intuitionist necessity modalities.

Our investigations are inspired by noninteference theorems for monads (logically speaking, the "says" modality from logics for access control). However, to the best of our knowledge, noninterference has not been investigated for comonads. Perhaps because the necessity and says modality are not logical duals,our proof incorporates some novelties; we use normal forms for intuionist S4 that are inspired by game semantics.

Our desire is to ultimately build a similar metatheory for a modal logic that incorporates *both* monads and comonads. Such logics are already used for security policies [9, 8] and type theories for functional languages already include both monads and comonads.

On the one hand, the game semantics for indexed monads [5] can be readily adapted to the current paper. However, it is unclear how to directly adopt this semantic approach to includes both indexed comonads and monads.

This state of current knowledge motivates the development of proof-theoretic techniques in this paper for indexed necessity modalities. A first comparison of the techniques used in this paper and in the literature on monads suggests that they are not incompatible, making us hopeful about future work on a general noninterference theorem for a full intuitionist logic with both necessity and says modalities. The development of a model theory based on game semantics for such a logic is also a topic of future work.

In that context, we intend to explore classical versions of indexed indexed modalities. In the monadic case the mixture of classical and monadic features leads to considerable collapse (if "A says s" then "s" or "A says false") [2]; however, the known properties of classical S4 suggest that non-trivial non-interference properties still could hold in the classical case.

This research was supported by NSF CCF-0915704.

References

1 Martín Abadi. Access control in a core calculus of dependency. *Electr. Notes Theor. Comput. Sci.*, 172:5–31, 2007.

2 Martín Abadi. Variations in access control logic. In Ron van der Meyden and Leendert van der Torre, editors, *DEON*, volume 5076 of *Lecture Notes in Computer Science*, pages 96–109. Springer, 2008.

3 Martín Abadi, Anindya Banerjee, Nevin Heintze, and Jon G. Riecke. A core calculus of dependency. In *POPL*, pages 147–160, 1999.

4 Martín Abadi, Michael Burrows, Butler W. Lampson, and Gordon D. Plotkin. A calculus for access control in distributed systems. *ACM Trans. Program. Lang. Syst.*, 15(4):706–734, 1993.

5 Samson Abramsky and Radha Jagadeesan. Game semantics for access control. *Electr. Notes Theor. Comput. Sci.*, 249:135–156, 2009.

6 Natasha Alechina, Michael Mendler, Valeria de Paiva, and Eike Ritter. Categorical and kripke semantics for constructive s4 modal logic. In Laurent Fribourg, editor, *CSL*, volume 2142 of *Lecture Notes in Computer Science*, pages 292–307. Springer, 2001.

7 G M Bierman and V C V de Paiva. On an intuitionistic modal logic. *Studia Logica*, 65:2000, 2001.

8 Henry DeYoung, , and Frank Pfenning. Reasoning about the consequences of authorization policies in a linear epistemic logic. Technical Report 1213, Computer Science Department, Carnegie Mellon University, 2009.

9 Deepak Garg, Lujo Bauer, Kevin D. Bowers, Frank Pfenning, and Michael K. Reiter. A linear logic of authorization and knowledge. In Dieter Gollmann, Jan Meier, and Andrei Sabelfeld, editors, *ESORICS*, volume 4189 of *Lecture Notes in Computer Science*, pages 297–312. Springer, 2006.

10 Deepak Garg and Frank Pfenning. Non-interference in constructive authorization logic. In *CSFW*, pages 283–296, 2006.

11 Jean Goubault-Larrecq and Eric Goubault. On the geometry of intutionist s4 proofs. *Homology, Homotopy and Applications*, 5(2):137–209, 2003.

12 G. E. Hughes and M. J Cresswell. *An introduction to modal logic*. 1972.

13 Gregory Malecha and Stephen Chong. A more precise security type system for dynamic security tests. In *Proceedings of the 5th ACM SIGPLAN Workshop on Programming Languages and Analysis for Security*, PLAS '10, pages 4:1–4:12, New York, NY, USA, 2010.

14 Aleksandar Nanevski. A Modal Calculus for Exception Handling. In *Intuitionistic Modal Logics and Applications Workshop (IMLA '05)*, Chicago, IL, June 2005.

15 Tomas Petricek, Dominic Orchard, and Alan Mycroft. Coeffects: typing context-dependent computations using comonads, 2012. `http://www.cl.cam.ac.uk/~tp322/papers/coeffects-flops.html`.

16 Frank Pfenning and Hao-Chi Wong. On a modal λ-calculus for S4. In *Proceedings of the Eleventh Conference on Mathematical Foundations of Programming Semantics*, New Orleans, Louisiana, March 1995. *Electronic Notes in Theoretical Computer Science*, Volume 1, Elsevier.

17 Stephen Tse and Steve Zdancewic. Translating dependency into parametricity. In *Proceedings of the ninth ACM SIGPLAN international conference on Functional programming*, ICFP '04, pages 115–125, New York, NY, USA, 2004.

18 Frank Wolter and Michael Zakharyashev. Intuitionistic modal logic. Technical report, The Institute of Computer Science, University of Leipzig, 1999. To appear in Logic in Florence, 1995.